Award Continuation Page
Login.Gov Identity Proofing/Verification and Fraud Detection

CONTRACT LINE ITEMS (CLINs)

Base Period
CLIN 0001

Estimated Transaction Volume	Base Transactions	(b) (4)
	FraudIQ Phone Verification	(b) (4)
	FraudIQ Facial Authentication	(b) (4)
	FraudIQ Auth Device (Logins/Low Risk)	(b) (4)
	FraudIQ Auth Device (Registrations/High Risk)	(b) (4)
	OTP via USPS Mail	(b) (4)

Estimated Unit Price	Base Transactions	(b) (4)
	FraudIQ Phone Verification	(b) (4)
	FraudIQ Facial Authentication	(b) (4)
	FraudIQ Auth Device (Logins/Low Risk)	(b) (4)
	FraudIQ Auth Device (Registrations/High Risk)	(b) (4)
	OTP via USPS Mail	(b) (4)

CLINs	CEILING
CLIN 0001 - Identity Proofing Services in support of Task 1, Service Requirement in accordance with Section 2.0 in the SOO	(b) (4)
CLIN 0002 - Implementation Fee	(b) (4)
CLIN 0003 - Initial Solution Consulting	(b) (4)
CLIN 0004 - Follow-on Solution Consulting	(b) (4)

Base Period Total Ceiling Price	(b) (4)

Option Period I

CLIN 1001

Estimated Transaction Volume	Base Transactions	(b) (4)
	FraudIQ Phone Verification	(b) (4)
	FraudIQ Facial Authentication	(b) (4)
	FraudIQ Auth Device (Logins/Low Risk)	(b) (4)
	FraudIQ Auth Device (Registrations/High Risk)	(b) (4)
	OTP via USPS Mail	200,000

Estimated Unit Price	Base Transactions	(b) (4)
	FraudIQ Phone Verification	(b) (4)
	FraudIQ Facial Authentication	(b) (4)
	FraudIQ Auth Device (Logins/Low Risk)	(b) (4)
	FraudIQ Auth Device (Registrations/High Risk)	(b) (4)
	OTP via USPS Mail	(b) (4)

CLINs	CEILING
CLIN 1001 - Identity Proofing Services in support of Task 1, Service Requirement in accordance with Section 2.0 in the SOO	(b) (4)
CLIN 1002 - Implementation Fee	(b
CLIN 1003 - Initial Solution Consulting	(b
CLIN 1004 - Follow-on Solution Consulting	(b) (4)

Option Period I Total Ceiling Price	(b) (4)

Total (Base Period – Option Period I): (b) (4)

*** Note 1:** The volume tier for pricing at the beginning of the period of performance will apply to all transactions for the period of performance – in this case the 8-month Base Period plus the 4-

month Option Period. For example, if the 2,000,001 – 5,000,000 tier is selected, all transactions would be billed at $0.27. At the end of the period of performance, if GSA has not met the minimum transaction volume for the selected volume tier (2,000,001 in this example), Equifax would bill for the difference in actual transaction volume and minimum transaction volume at the selected volume tier price ($0.27 in this example).

1.0 BACKGROUND

Login.Gov (formerly Connect.Gov) is a government-wide, cloud-based "Federated Digital Identity Ecosystem" that enables federal agencies to leverage government-provided digital consumer credentials with greater privacy, security and convenience for consumers. The proposed new acquisitions would provide identity service components for integration into the Login.Gov Shared Authentication Platform, which will replace the contracts currently used to operate the Initial Operational Capability (IOC) phase, and establish the Full Operational Capability (FOC) phase of the program. The FOC will enable a greater number of customer agencies to utilize the program without the need of developing, procuring, and managing user identities. Furthermore, they can leverage and meet the guidelines for shared services and benefit from volume pricing and better cost estimations.

In February 2012, the White House established the Federal Cloud Credential Exchange (FCCX), known as Connect.Gov in the IOC phase, to investigate the potential for a common solution for federated identity and credential exchange across government agencies.

The IOC phase, known as Connect.Gov, provides a secure, privacy-enhancing service that conveniently connects people to online government services and applications using an approved digital credential they may already have and trust. Connect.Gov allows an individual to access agency websites and services by signing in with an approved third-party sign-in partner, thereby eliminating the need for consumers to maintain multiple logins for government agencies. General Services Administration (GSA)/Technology Transformation Service (TTS) manages Connect.Gov and is responsible for the governance structure and business relationships with agencies, industry and Credential Service Providers (CSPs). The United States Postal Service (USPS) serves as the technology manager and is the entity responsible for providing the operating platform for Connect.Gov.

The FAS ITS Cloud Computing Services Program Management Office (CCS PMO) and the Technology Transformation Service (TTS) and 18F are working together to move the Program from its IOC phase (Connect.Gov) to the FOC phase (Login.Gov), which will be an enterprise class, cloud-based service that can provide all Government agencies with the ability to provide their users with digital consumer identities. Based on lessons learned from the IOC and a focus on improving agency and consumer usability, 18F is building a Shared Authentication Platform with a modular technical architecture that will consist of different component services which allow for agile and fast modifications to meet agency needs and industry standards.

18F and CCS PMO are collaborating to define and acquire with this acquisition one of these component services, namely *Identify Proofing/Verification and Fraud Detection*, which will be integrated into the Login.Gov FOC.

2.0 OBJECTIVES

The Login.Gov Program is undergoing significant modifications in direct response to recent laws passed in Congress and executive orders released by the Executive Office of the President instructing federal agencies to protect citizen data in transactions with the Government:

- The Cybersecurity Information Sharing Act (CISA) passed in October 2015;
- The Cybersecurity National Action Plan (CNAP) released in March 2016 by the Executive Office of the President to identify short- and long-term actions to meet CISA; and
- The Implementation Plan Draft released in April 2016 as a plan for action to Executive Order 13681 - Improving the Security of Consumer Financial Transactions.

The acquisition of the following consumer identity service components which will be integrated by 18F into the Login.Gov Shared Authentication Platform via application program interfaces (APIs):

- *Identity Proofing/Verification and Fraud Detection*
  Identity proofing and verification is a service that verifies an individual's identity based on historical life or aggregated transactional information obtained from public and proprietary data sources. Consumer fraud detection service identifies and detects stolen identities and fraud using behavioral algorithms and device intelligence such as reputation, velocity, geolocation, cloaking, and other relational anomalies with real-time transaction analysis.

The objective of this task is for the Contractor to provide GSA TTS access to data and services via API in order to proof user identity online and to assist in ongoing identity verification and validation in compliance with NIST Level of Assurance 3 as defined in 800-63-2.

3.0 ROLES & RESPONSIBILITIES

Contracting Officer (CO):

The CO is responsible for monitoring call order contract compliance, contract administration, and cost control and for resolving any differences between the observations documented by the Government and the contractor. The CO will designate, at a minimum, one (1) CO's Representative (COR) and one (1) Alternate CO's Representative (ACOR) as the Government authority for performance management. The number of additional representatives serving as technical inspectors depends on the complexity of the services measured, as well as the contractor's performance, and must be identified and designated by the CO.

Contracting Officer's Representative and Alternate Contracting Officer's Representative:

The COR and the ACOR are designated in writing by the CO to act as his or her authorized representative to assist in administering a contract. COR/ACOR limitations are contained in the written appointment letter. The COR/ACOR are responsible for technical administration of the project and ensures proper Government surveillance of the contractor's performance. The COR/ACOR are not empowered to make any contractual commitments or to authorize any contractual changes on the Government's behalf. Any changes that the contractor deems may affect contract price, terms, or conditions shall be referred to the CO for action. The COR/ACOR will have the responsibility to document the inspection and evaluation of the contractor's work performance. The COR/ACOR's acceptance of the vendor product is dependent on the Product Owner's approval.

Procurement Project Manager:

The Procurement Project Manager is the interface between the requiring organization (GSA 18F) and contracting organization (GSA FAS AAS/NCR). The Procurement PM coordinates technical aspects of the contract with the COR/ACOR and CO, assists with contract administration, ensures client acceptance of services, and reviews invoices for payment.

18F Product Lead:

The 18F Product Lead is responsible for coordination between the contractor, the Product Owner, as well as the CO and COR/ACOR.

18F Technical Lead:

The 18F technical lead is responsible for coordination between the contractor's development team, the Product Owner and the key interagency stakeholders.

Product Owner:
The Product Owner is the project's key stakeholder. They are responsible for having a vision of what he or she wishes to build, and convey the vision to the 18F Product Lead and the contractor's scrum or development team. The Product Owner does this in part through the product backlog, which will be a prioritized features list for the product. The Product Owner is responsible for advocating on behalf of the agency's needs and responsible for decision-making during sprint planning and implementation. The Product Owner will work with the COR/ACOR to inspect vendor work

4.0 TASKS

4.1 TASK 1: IDENTITY PROOFING/VERIFICATION & FRAUD DETECTION PRODUCT(S)

The objective of this task is for the Contractor to provide GSA TTS access to data and services via Application Program Interface (API) in order to proof user identity online and to assist in ongoing identity verification and validation. GSA TTS seeks data products and capabilities such as:

- Verify address of record matches asserted address
- Financial data validation (e.g., checking, savings, loans, credit cards, utility account data)
- Other methods of identity validation
- Consumer fraud detection service that identifies and detects stolen identities, synthetic and true name fraud etc. using behavioral algorithms, device intelligence such as reputation, velocity, geolocation, cloaking and other relational anomalies with real-time transaction analysis

The Contractor shall outline their approach to meet this objective and provide a technical description with steps of how their system works along with visuals such as data flow, sequence diagram, code examples, high level architecture etc. Ideally the Contractor should provide procedural, cookbook-style documentation and examples of specific sequences, flows and steps.

In addition, the Contractor shall specify their compliance with the following set of requirements using the attached spreadsheet "Attachment A - IDP Requirements" and fill out attached Attachment B- Proofing Sources" spreadsheet with all attributes that are contained within its data sources. The Contractor shall outline its approach and roadmap that demonstrates its understanding and roadmap items to update its service based on NIST 800-63-3 Draft for IAL 2.

The following table includes all requirements the Contractor shall provide and the priority level:

ID	Requirement	Priority
Coverage & Resolution		
1	Identity data sources that may include but aren't limited to FCRA and non-FCRA data sources, public records, utility data, employment/ income details provided directly by employers, credit bureau information, phone records, etc.	Must Have
2	Cover 75% of U.S. population for resolution	Must have

3	Ability to deliver at a minimum, dynamic combinations of the following attributes to resolve an identity to a single record: ● Legal First Name and Last Name ● Middle Name or Initial ● Current Address: (Parsed and Full) ● Date of Birth: (Parsed and Full) ● Social Security Number: (Parsed and Full) ● Phone Number ● Email Address	Must have
Validation		
4	Ability to provide Out of Wallet Support-Online	Must Have
5	Users should only need to enter data once in the proofing flow and should not need to re-enter information unless needed for business reasons	Must Have
6	Ability to provide Identity Verification via APIs	Must Have
7	Ability to resolve a single record with a true positive and negative result	Must have
8	Ability to calculate & assign a riskiness score to a single record	Must have
9	Ability to return verbose, granular feedback for pass/fail at each step of the proofing process to help improve and tune pass rates. Demonstrated understanding and ability to categorize as statistically relevant ways utilizing standard scientific method practices. Examples are categorizing data as true positive, false positive, true negative, false negative.	Must have
Fraud Detection		
10	Ability to conduct real-time transaction analysis for potentially fraudulent events and both log events and adjust the proofing flow on a transactional basis	Must Have

11	Ability to identify fraudulent activity trends using behavioral algorithms, relational anomalies and other statistical and machine learning techniques	Must Have
12	Record and report on input velocity	Must have
Logging & Reporting		
13	Ability to provide monthly status report as specified	Must Have
14	Ability to provide a maintenance schedule detailing any infrastructure, software or data updates and upgrades, duration, impact on Login.Gov, expected downtime etc.	Must Have
15	Log points of failure and provide regular reports on that	Must Have
16	Ability to export all reports and transactional logs in .CSV format	Must Have
User Experience		
17	Support for English language	Must have
18	Contractor identity solutions comply with Section 508 Requirements	Must have
Other Requirements		
19	Ability to work with GSA TTS to improve the identity proofing process and outcomes	Must Have
20	Ability to provide test environment, pre-built unit tests, and other relevant documentation to help develop and test the service	Must Have

21	Conforms to NIST LOA3 as defined in NIST 800-63-2	Must-have
General		
22	Ability to provide detailed raw log information regarding system events, transactions, in a standard format (such as .CSV, pipe, line delimited) with standardized delivery to be determined mutually with the Government	Must have
23	Notify GSA TTS of changes to the identity service component, such as changes to the capabilities, service workflows, the API, interface data specifications, and data sources	Must have
24	Maintain test environments to allow for separation of real test data with the ability for the Government to conduct end-to-end testing that are a mirror of production	Must have
25	Maintain a sandbox environment to allow testing technologies under development	Must have
26	Conduct testing with GSA TTS to include: systems integration, performance, security, and user acceptance	Must have
27	Deliver Systems Interface Specifications document following successful integrations to production and update document as needed	Must have
28	Deliver Procedural Setup Guide following successful integrations to production and update guide as needed	Must have
29	Follow a roadmap to update its service based on NIST 800-63-3	Must have

As a regular part of Identity Proofing/Verification & Fraud Detection Product(s), the Contractor shall also provide the following:

- **Routine Operations & Maintenance:**

The Contractor shall provide operations and maintenance activities associated with the on-going support related to the performance of routine, preventive, predictive, scheduled, and unscheduled actions aimed at preventing credential authentication solution failure and increasing efficiency and reliability on a continuous basis. Contractor shall correct errors and bugs/defects identified during operations on a prioritized basis. The priority and urgency of fixes will be determined by GSA TTS and Contractor's QA staff, in accordance with established processes and standards.

- **Incident Resolution:**
  The Contractor shall provide support to investigate, assess, and diagnosis reported incidents and technical problems. Contractor shall maintain the operational status of the solution, trace down potential problems, fix defects and work with GSA TTS to maintain operations and throughput. Contractor shall take appropriate remediation actions to expedite the operational recovery and closure of incidents.

- **Updates & Modifications:**
  The Contractor shall make minor modifications to the solution if changes in shared authentication platform business processes or available hardware necessitate them. In addition, the Contractor shall perform updates to existing user documentation to reflect changes made based on bug fixes, release updates, and system maintenance.

- **Service Level Agreement:**
  The Contractor shall provide a copy of its Service Level Agreement (SLA) and specify their compliance to performance requirements via attached SLA Requirements sheet.

- **Technical Support:**
  The Contractor shall provide Tier 2, Tier 3 technical support post integration and work with GSA TTS to troubleshoot, fix and resolve any technical issues involving their service in accordance with defined performance requirements.

- **Operational Reports**
  The Contractor shall deliver a Monthly Status Report. These reports must provide accurate, timely, and complete information supporting reporting requirements. The Monthly Status Report must include the following data elements at a minimum:
    - Total and monthly transactions, proofing success/failure rate, causes of error, fraudulent attempts, reproofing rate, demographics and any other data useful for GSA TTS to make informed decisions on tweaking and improving proofing rate and security of Login.Gov platform
    - Performance Statistics associated with meeting the Performance Requirements
    - Identification of any issues impacting the ability of the provided services, accompanied by possible solutions
    - Status on previously identified issues as well as actions taken to mitigate the situation and/or progress made in rectifying the situation
    - The format will be decided during contract kickoff and discussion between Contractor and the Government

- The report shall be delivered no later than five business days after the end of the month

4.2 TASK 2: IMPLEMENTATION FEE

Contractor shall provide application integration and configuration support activities during the initial service setup & implementation of Contractor products supplied under Task One.

4.3 TASK 3: INITIAL SOLUTION CONSULTING

Contractor shall assist GSA TTS staff in implementing an optimal configuration of workflow, thresholds, fraud detection algorithms etc. based on its prior experience, best practices and subject matter expertise (SME). In addition the Contractor shall provide the testing, tuning and risk leveling of Contractor services to meet GSA TTS business requirements post initial application integration. The Government expects Contractor staff to perform the work primarily onsite at GSA TTS Headquarters. Contractor staff may also work at Contractor facilities at Government's discretion. The Government estimates 1 FTE will be required for a three to six month period. The actual position needed is dependent on which task is being worked on and will be discussed between the Government and Contractor. The solutions consultant team should be experienced at translating business needs to vendor solutions that satisfy those needs.

4.4 TASK 4: FOLLOW ON SOLUTION CONSULTING

Once Login.Gov goes live, the Contractor shall participate in periodic reviews of proofing pass/ fail rates and other performance metrics, and tuning exercises in order to improve proofing rates. This will involve the analysis of system configuration, reports, creation of recommendations to improve the results and the underlying identity model, actual changes to the system and the Identity model(s) and supporting structure. The reviews and resulting changes will occur at least every 30 days or at the Government's discretion less often. The success/ failure rate reports will be required across multiple dimensions including not limited to age, geography, income, etc.
In addition to Monthly Status Reports, the Contractor shall provide a maintenance schedule. The Contractor shall provide direct POCs that GSA TTS can contact with questions or issues regarding the Contractor's services & solution. Contractor shall continuously monitor performance and report any deviation from previous Monthly Status Report or Task Monitoring meetings.

SYSTEM SECURITY

The Contractor shall be subject to all applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements.

The Contractor shall comply with Federal Information Security Management Act (FISMA) associated guidance and directives to include Federal Information Processing Standards (FIPS), NIST Special Publication (SP) 800 series guidelines (available at: http://csrc.nist.gov/), GSA

TTS IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of Government IT. Compliance references include:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information Security) available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf
- Privacy Act of 1974 (5 U.S.C. § 552a)
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors," August 27, 2004; available at: http://www.idmanagement.gov/
- OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." (Available at: http://www.whitehouse.gov/omb/memoranda_2004)
- OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors"
- OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems"
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems"
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules"
- NIST Special Publication 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems"
- NIST Special Publication 800-30 Revision 1, "Guide for Conducting Risk Assessments"
- NIST Special Publication 800-34 Revision 1, "Contingency Planning Guide for Federal Information Systems"
- NIST SP 800-41, Revision 1, "Guidelines on Firewalls and Firewall Policy"
- NIST SP 800-37, Revision 1, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach"
- NIST Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems"

- NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations”
- NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans”
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling ll Guide”
- NIST Special Publication 800-88 Revision 1, “Guidelines for Media Sanitization”
- NIST Special Publication 800-128, “Guide for Security-Focused Configuration Management of Information Systems”
- NIST Special Publication 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations”
- NIST SP 800-160 “Systems Security Engineering” Draft
- NIST SP 800-63-2 “Electronic Authentication Guideline”

Despite enhanced security controls and monitoring, incidents may occur that require immediate response from the Contractor. Incidents could include misuse, fraud, misappropriation, espionage, sabotage, and inadvertent or deliberate compromise of the shared authentication platform. The Contractor shall identify proposed plans, communications and protocols for responding to security and privacy incidents in collaboration with the Government. The Contractor shall comply with incident reporting requirements outlined in NIST SP 800-61 and the U.S. Computer Emergency Readiness Team US-CERT.

Upon termination or expiration of the contract, once all data is provided back to the Federal Government the Contractor shall discard all Government data according to Federal regulations, and must certify no Government data has been retained unless otherwise authorized.

The Government will retain unrestricted rights to Government data. The data shall be available to the Govt. upon request within one business day or within the timeframe specified otherwise in the Government’s request, and shall not be used for any other purpose other than that specified herein. The Contractor shall provide requested data at no additional cost to the Government.

No data related to the work under this contract shall be released by the Contractor without the consent of the Government in writing. All requests for release must be submitted in writing to the COR/CO.

The Contractor shall not disclose sensitive or proprietary information pertaining to GSA TTS or any of its operating units, the U.S. Government, industry, business partners, or consumers to any unauthorized persons. The Contractor shall be subject to any and all penalties imposed by law for unlawful disclosure of sensitive information.

The Contractor shall immediately notify, in writing, GSA TTS upon discovery of any inadvertent or deliberate disclosures of information other than those pursuant to performing the work under the contract. The Contractor shall work with GSA TTS and make available its resources to work

with GSA TTS and other entities to resolve this issue.

The Contractor shall retain any PII consent logs created pursuant to this contract and transfer the logs to GSA TTS at the expiration of the contract.

AUDIT

The Contractor shall allow GSA TTS to conduct operational and security audits to verify the Contractor's compliance with our SLAs and security standards. The audits will be conducted following these guidelines:

GSA TTS may perform one audit yearly, and may conduct additional audits after a confirmed security breach (one audit per breach). The Contractor shall accommodate assessments by GSA TTS when requested. Unannounced assessments are required to occur within ten business days from initial notification.

- The Contractor shall make a good-faith effort to answer any questions GSA TTS has, and to give access to requested information (under suitable non-disclosure agreements (NDAs), if necessary). The Contractor shall provide up to 40 hours of staff time per audit; any further time is at the Contractor's discretion and may be billed at the Contractor's professional services rate.
- Audits will be conducted remotely; no on-site visits will be required (in either direction).
- Any issues discovered by the audit shall be remediated by the Contractor in a mutually-agreed-upon timeframe.

The Contractor shall provide GSA TTS with any applicable documentation of their security stance and compliance achievements. Examples include:

Internal security architecture documentation

- Internal security policies and procedure documentation
- Security compliance reports, such as PCI, SOC 2/3, SIG, CSA CSQ, etc.

SECURITY OF DATA INCLUDING PERSONALLY IDENTIFIABLE (PII) DATA

- A breach is defined as the actual or possible loss of control, unauthorized disclosure, or unauthorized access, whether physical or electronic, of data from the Contractor's systems that was transmitted as part of the assertion for identity resolution, in any location that is within the control of the Contractor including the underlying identity verification data sources, where persons other than authorized users gain access or potential access to such information for other than authorized purposes where one or more individuals will be adversely affected.
- By acceptance of, or performance on, this contract, the Contractor agrees that in the event of any actual or suspected breach of as defined in paragraph (1) above, the Contractor shall immediately (and in no event later than within one hour of discovery) report the breach to the GSA TTS Contracting Officer (CO) or the Contracting Officer's

Representative (COR), the specified contact for the General Services Administration Incident Response Team, and the US Computer Emergency Readiness Team (US CERT) (http://www.us-cert.gov/). If the breach occurs outside of regular business hours and/or neither the CO nor the COR can be reached, Contractor shall call the phone numbers as specified by the CO or the COR and GSA TTS points of contact (POCs) for emergency contacts outside of business hours within one hour of discovery of the breach. Contractor shall also notify the CO and COR as soon as possible during regular business hours.

- In the event of the actual or possible loss of control, unauthorized disclosure, or unauthorized access, whether physical or electronic, in locations controlled by the Contractor, of personal information about End consumers of the Login.Gov service that were not transmitted as part of the assertion for identity resolution, Contractor shall notify GSA TTS at the earliest opportunity during regular business hours.
- Contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification to End consumers as a result of a breach as defined in paragraph (1) above shall be coordinated with GSA TTS. The method and content of any notification by Contractor as a result of a breach as defined in paragraph (1) above will be subject to the approval of GSA TTS. In the event of a breach as defined in paragraph (1) above, Contractor assumes full responsibility for taking corrective action consistent with GSA Data Breach Notification Procedures (http://www.gsa.gov/portal/directive/d0/content/675850).
- Contractor also agrees to cooperate fully with the CO, the GSA TTS Inspector General, and any other authorized Government investigator during any investigation regarding a breach or suspected breach of personally identifiable information as defined in paragraph (1) above. This cooperation includes providing access to documents and systems for a forensic investigation such as systems logs and server images, to determine how or why the breach occurred and how to prevent a similar occurrence in the future. Contractor shall also correct, at its own cost, the system or protocol to prevent any future similar breach.
- The Contractor further certifies that it has a security policy in place that contains procedures to promptly notify any individual whose personally identifiable information (as defined by OMB) was, or is reasonably believed to have been, breached. Any notification to End consumers as a result of a breach as defined in paragraph (1) above shall be coordinated with GSA TTS. The method and content of any notification by the Contractor as a result of a breach as defined in paragraph (1) above will be subject to the approval of GSA TTS. In the event of a breach as defined in paragraph (1) above, the Contractor shall assume full responsibility for taking corrective action consistent with GSA Data Breach Notification Procedures

  (http://www.gsa.gov/portal/directive/d0/content/675850).

FOUR- PERSONALLY IDENTIFIABLE INFORMATION (PII) NOTIFICATION REQUIREMENT

The Contractor shall have in place procedures and the capability to promptly notify any individual whose PII/Sensitive PII was, or is reasonably believed to have been, breached, as determined appropriate by GSA. The method and content of any notification by the Contractor

shall be coordinated with, and subject to the prior approval of GSA, based upon a risk-based analysis conducted by GSA in accordance with GSA Privacy incident Handling Guidance and GSA Privacy Incident Standard Operating Procedures. Notification will not proceed unless GSA has determined that: (1) notification is appropriate; and (2) would not impede a law enforcement investigation or jeopardize national security.

Subject to GSA analysis of the breach and the terms of its instructions to the Contractor regarding any resulting breach notification, a method of notification may include letters to affected individuals sent by first class mail, electronic means, or general public notice, as approved by GSA. At minimum, a notification should include: (1) a brief description of how the breach occurred; (2) a description of the types of personal information involved in the breach; (3) a statement as to whether the information was encrypted or protected by other means; (4) steps an individual may take to protect themselves; (5) what the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and (6) point of contact information identifying who affected individuals may contact for further information. The Contractor agrees to assist in and comply with PII/Sensitive PII incident remediation and/or mitigation efforts and instructions, including those breaches that are not a result of the Contractor or employee actions, but the Contractor is an unintentional recipient of privacy data. Actions may include allowing GSA incident response personnel to have access to computing equipment or storage devices, complying with instructions to remove emails or files from local or network drives, mobile devices (BlackBerry, Smartphone, iPad, USB thumb drives, etc...). In the event that a PII/Sensitive PII breach occurs as a result of the violation of a term of this contract by the Contractor or its employees, the Contractor shall, as directed by the contracting officer and at no cost to GSA, take timely action to correct or mitigate the violation, which may include providing notification and/or other identity protection services to affected individuals for a period not to exceed 24 months from discovery of the breach. Should GSA elect to provide and/or procure notification or identity protection services in response to a breach, the Contractor shall be responsible for reimbursing GSA for those expenses. To ensure continuity with existing Government identity protection and credit monitoring efforts, the Contractor shall use the identity protection service provider specified by GSA.

5.0 POST AWARD ORIENTATION CONFERENCE

The Government's team, CO, COR/ACOR, the 18F Product Lead and the Product Owner will hold a Kick-Off Meeting/Post-Award Conference with the contractor. This will be done virtually with the contractor’s team and other relevant Government staff to review and clarify the project’s objectives, expectations from the Government, and address any questions the contractor may have.

The Kick-Off Meeting/Post-Award Conference will take place within 10 calendar days from award. The contractor shall provide any finalized contractor Teaming Arrangements (CTAs)/Subcontractor arrangements at this time.

6.0 OPERATIONAL REQUIREMENTS

6.1 GSA AAS BUSINNES SYSTEMS (AASBS) WEB PORTAL

The GSA AASBS (Assisted Acquisition Services Business Systems) also known as IT Solutions Shop (ITSS) web portal will be accessible to the contractor during the performance of the call order and be used in the administration of the call order. This web-based system at https://portal.fas.gsa.gov/web/guest shall be used by the contractor to upload status reports, deliverables, invoices, and to respond to inquiries. Contractor shall maintain a current count on this system.

6.2 DELIVERABLES

The following schedule of milestones will be used by the COR to monitor timely progress under this Contract. Deliverables are due the next Government workday if the due date falls on a holiday or weekend. The contractor shall deliver the deliverables listed in the following table:

Item #	Title	Description	Delivery Media and Requirements	Delivery Frequency and/or Due Date
1	Test/Sandbox Environment		Online web access	Throughout Period of Performance
2	API Documentation		Email or online web Access	Throughout Period of Performance
3	Monthly Status Report		Email	Monthly
4	Maintenance Schedule		Email	As needed
5	Change, Incident and Problem Management	A plan that states the processes, procedures, standards, documentation, controls, and management of all changes on the project and contract	Via email to COR and designated GSA TTS POCs	Within 15 business days after contract award

6	Test Case Documentation	Test data scripts and scenarios necessary to support integration testing	Via email to COR and designated GSA TTS POCs	Within 15 business days after Kick Off Meeting and as required to support integration testing
7	Test Results	Report findings and incidents based on integration testing	Via email to COR and designated GSA TTS POCs	Within 5 days of completing a round of integration testing

6.2.1 PACKAGING AND MARKING

The contractor shall provide delivery of electronic copies of progress reports and deliverable completion documentation. Electronic copies shall be delivered via email attachment, IT-Solutions Shop (ITSS) or other media by mutual agreement of the parties.

All final reports and deliverable completion documents should be submitted electronically through GSA's electronic Contract system (ITSS) at:

ITSS https://web.itss.gsa.gov/login

NOTE: FAILURE TO SUBMIT THE REPORTS/DELIVERABLES IN ITSS WILL RESULT IN REJECTION OF THE REPORT/DELIVERABLE.

6.2.2 PACKAGING

All reports and deliverables that are in hard copy format, as opposed to electronic format, and that are physically transported through the U.S. mail or private courier services, are to be securely packaged using the contractor’s best practices.

6.2.3 MARKING

All reports and deliverables that are in hard copy format, as opposed to electronic format, and that are physically transported through the U.S. mail or private courier services, are to be addressed to the individual at the office or floor at the end destination, with the outside package clearly marked to indicate the order number and the recipient's office telephone number.

6.2.4 PLACE OF INSPECTION AND ACCEPTANCE

Inspection and acceptance of all work performance, reports, and other deliverables under this Contract shall be performed by the GSA COR within five working days after receipt of deliverable.

6.2.5 SCOPE OF INSPECTION

All deliverables will be inspected for content, completeness, accuracy, and conformance to requirements by the GSA COR. Inspection will include, if deemed necessary by the Government, validation of information or software through the use of automated tools, testing, or inspections of the deliverables, as specified in the Contract. The scope and nature of this inspection will be sufficiently comprehensive to ensure the completeness, quality, and adequacy of all deliverables.

The Government requires a period NTE 15 workdays after receipt of final deliverable items for inspection and acceptance or rejection.

6.2.6 BASIS OF ACCEPTANCE

The basis for acceptance shall be compliance with the requirements set forth in the Contract, the contractor's quote, and relevant terms and conditions of the contract. Deliverable items rejected shall be corrected in accordance with the applicable clauses.

For IT development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government are resolved, through documentation updates, program correction, or other mutually agreeable methods.

Reports, documents, and narrative-type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government are corrected.

If the draft deliverable is adequate, the Government has the option to accept the draft and provide comments for incorporation into the final version. All of the Government's comments on deliverables must either be incorporated in the succeeding version of the deliverable, or the contractor must demonstrate to the Government's satisfaction why such comments will not be incorporated.

If the Govt. finds that a draft or final deliverable contains spelling errors, grammatical errors, or improper format, or otherwise does not conform to the requirements stated within this Contract,

the document may be immediately rejected without further review and returned to the contractor for correction and resubmission. If the contractor requires additional Government guidance to produce an acceptable draft, the contractor shall arrange a meeting with the GSA COR.

For IT development, the final acceptance will occur when all discrepancies, errors, or other deficiencies identified in writing by the Government have been resolved, through documentation updates, program correction, or other mutually agreeable methods.

6.2.7 DRAFT DELIVERABLES

The Govt. will provide written acceptance, comments, and/or change requests, if any, within 5 workdays (unless specified otherwise in Section 5) from Govt. receipt of the draft deliverable. Upon receipt of the Govt. comments, the contractor shall have ten workdays to incorporate the Government's comments and/or change requests and to resubmit the deliverable in its final form.

6.2.8 WRITTEN ACCEPTANCE/REJECTION BY THE GOVERNMENT

The GSA CO/COR will provide written notification of acceptance or rejection of all final deliverables within 15 workdays unless specified otherwise in Section 5. All notifications of rejection will be accompanied with an explanation of the specific deficiencies causing the rejection.

6.2.9 NON-CONFORMING PRODUCTS OR SERVICES

Non-conforming products or services will be rejected. Deficiencies will be corrected, by the contractor, within five workdays of the rejection notice. If the deficiencies cannot be corrected within ten workdays, the contractor shall immediately notify the GSA COR of the reason for the delay and provide a proposed corrective action plan within ten workdays.

6.2.10 DELIVERY INSTRUCTIONS

The contractor shall deliver all electronic versions by email and removable electronic media. The following are the required electronic formats unless stated otherwise, whose versions must be compatible with the latest, commonly available version on the market.

a. Text	MS Word
b. Spreadsheets	MS Excel
c. Briefings	MS PowerPoint
d. Drawings	MS Visio
e. Schedules	MS Project

Unclassified deliverables or correspondence shall be submitted electronically to the following website location: https://portal.fas.gsa.gov/

Copies of all deliverables shall also be delivered electronically to the TTS/18F Technical POC in a Microsoft format:

Jonathan Prisby, jonathan.prisby@gsa.gov, 202-394-2777

6.2.11 NOTICE REGARDING LATE DELIVERY/PROBLEM NOTIFICATION REPORT

The contractor shall notify the GSA COR via a Problem Notification Report (PNR) (Section 9) as soon as it becomes apparent to the contractor that a scheduled delivery will be late. The contractor shall include in the PNR the rationale for late delivery, the expected date for the delivery, and the project impact of the late delivery. The COR will review the new schedule and provide guidance to the contractor. Such notification in no way limits any Government contractual rights or remedies including, but not limited to, termination.

6.2.12 QUALITY ASSURANCE

Based on the QASP provided by the Government, the offeror shall provide any recommended revisions based on the solution proposed.

7.0 TERMS AND CONDITIONS

7.1 TYPE OF CONTRACT

The contractor shall perform the effort required by this Contract on a Time and Materials (T&M) and Firm Fixed Price (FFP) basis.

7.2 PERIOD OF PERFORMANCE (POP)

The POP includes a base period of 8 months, with 1 additional option period of 4 months.

7.3 PLACE AND HOURS OF PERFORMANCE

Place of performance is primarily at the contractor facility, however, CLIN 0003, most of the time will be spent at GSA Headquarters, 1800 F ST NW, Washington, DC as approved by the Government.

The normal operating hours at GSA Headquarters are from 9:00 AM to 5:00PM EST, Monday through Friday. The Contractor will not be required to report to GSA Headquarters on the following federal holidays:

New Year's Day	Birthday of Martin Luther King, Jr.
Washington's Birthday	Memorial Day

Independence Day	Labor Day
Columbus Day	Veterans Day
Thanksgiving Day	Christmas Day

The hours of operation while on the Contractor's facilities are to be determined by the contractor; however, the contractor is required to be present for a weekly meeting, either in person or over the phone, at the Government's discretion (to be determined after award).

While working at GSA Headquarters, the Contractor shall possess a current favorable National Agency Check (NAC) for unescorted access while in the building. Regardless of clearance level, the contractor shall maintain this clearance throughout the contract period of performance to provide support for multiple tasks and meetings.

Personal Identity Verification (PIV), building badges and security badges will be required in performance of each task and will be issued upon completion and clearance of a security background check. These items will be provided at no cost to the Contractor. If required, an interim clearance may be issued pending approval of final clearance. All items issued are to be returned at the completion of the contract or the employee's termination. Clearance must be obtained within 60 days after award.

7.4 ADMINISTRATION POINTS OF CONTACT

Contract Specialist (CS): Jasmine Mitchell, Federal Acquisition Service, GSA, jasmine.mitchell@gsa.gov

Contracting Officer (CO): Dan Higgins, Contracting Officer, Federal Acquisition Service, GSA, daniel.higgins@gsa.gov

CO's Representative (COR): Michelle McNellis, GSA, Technology Transformation Services, Michelle.Mcnellis@gsa.gov

Alternate CO's Representative (ACOR): Kirsten Green, GSA, Technology Transformation Services Kirsten.Green@gsa.gov

7.5 GOVERNMENT FURNISHED PROPERTY (GFP)

The Government will provide a space to work for all work when the Contractor is required to be at the Government's facilities. No other Government Property will be provided. The Contractor shall furnish all facilities, equipment and supplies to ensure successful performance under this Contract.

7.6 NON-PERSONAL SERVICES

This call order is not being used to procure personal services prohibited by FAR 37.104, Personal services contract.

7.7 PRIVACY ACT

Performance of this call order may require that personnel have access to Privacy Information. Contractor personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code, Section 552a and any other applicable rules and regulations.

7.8 SECTION 508 COMPLIANCE REQUIREMENTS

Section 508 of the Rehabilitation Act requires Federal agencies to make their electronic and information technology accessible to people with disabilities. This applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. All electronic and information technology (EIT) procured through this Contract must meet the applicable accessibility standards specified in 36CFR1194.2, unless an agency exception to this requirement exists. Any agency exceptions applicable to this Contract are listed below.

The standards define Electronic and Information Technology, in part, as "any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, or duplication of data or information. The standards define the type of technology covered and set forth provisions that establish a minimum level of accessibility. The application section of the standards (1194.2) outlines the scope and coverage of the standards. The standards cover the full range of electronic and information technologies in the Federal sector, including those used for communication, duplication, computing, storage, presentation, control, transport and production. This includes computers, software, networks, peripherals and other types of electronic office equipment.

7.9 NON-DISCLOSURE AGREEMENT

All contractor key personnel, employees, agents, subcontractors and subcontractor personnel who will have access to documents or data during the performance of their duties under the contract shall execute the attached Non-Disclosure Agreement and return it to the CO within 5 calendar days of award and before being given access to such information or documents.

a. The preliminary and final deliverables and all associated working papers and other material deemed relevant by GSA TTS that have been generated by the Contractor in the performance under this contract are the property of the U.S. Govt. and must be submitted to the GSA TTS COR at the conclusion of the order.
b. All documents produced for this project are the property of the U.S. Government and cannot be reproduced, or retained by the Contractor. All appropriate project documentation will be given to GSA TTS during and at the end of this contract. Contractor shall not release any information without the written consent of the Contracting Officer (CO). Any request for information relating to the contract presented to Contractor shall be submitted to the CO for approval for a response.

c. The Contractor shall not disclose sensitive or proprietary information pertaining to, or in the possession of, GSA TTS or any of its operating units, Government, industry, or business partners or customers to any unauthorized persons. Contractor shall be subject to any and all penalties imposed by law for unlawful disclosure of sensitive information.

8.0 INVOICING/PROCEDURES FOR PAYMENT

The period of performance for each invoice shall be for one calendar month. The contractor shall submit only one invoice per month per order/contract.

The Government reserves the right to audit, thus; the contractor shall keep on file all backup support documentation for travels as applicable.

8.1 INVOICE SUBMISSION

All Requests for Payments by the contractor shall include the following data elements to be considered proper for payment:

Task Order number: *(from GSA Form 1449, Block 4)*

Paying Number: *(ACT/DAC NO.) (From GSA Form 1449)*

NCR Project No.: ID11160060

Project Title: Login.Gov Identity Proofing/Verification and Fraud Detection

8.2 NCR INVOICE INSTRUCTIONS

A proper invoice shall be submitted monthly and not later than 5 work days after acceptance by the Govt. of the product, service, and/or cost item. A separate invoice for each Contract shall be submitted on official company letterhead with detailed costs for each of the following categories:

1. Total labor charges
2. Travel and per diem charges (if applicable)
3. Total invoice amount
4. Prompt payment discount offered (if applicable)

For other direct costs such as equipment, travel, per diem, subcontractor labor, etc., invoices shall reflect the contractor's actual expense for the item, plus General and Administrative charges (G&A) These charges shall not exceed limits specified in the Contract. No charges will be paid by the Government that are not specifically detailed in the Contract and specifically approved in the underlying contract. Copies of contractor paid invoices, receipts, and travel vouchers completed in accordance with Federal Travel Regulations (FTR) shall be maintained by the contractor and made available to the Government upon request.

In addition to the above information, the invoice shall include the following minimum task identification:

5. GSA Contract Number
6. Accounting Control Transaction (ACT) number (GSA Form 300, Block 4)
7. Period of Performance (month services performed for work request Contracts, month deliverable completed for fixed price Contracts).
8. Invoice Number
9. Client name and address

When the paying office is GSA, the original of each invoice, with supporting documentation, shall be submitted to the GSA Paying Office designated in Block 24 of the GSA Form 300.

In those cases where the paying office is other than GSA, the invoice/paying office will be as specified in the order. One additional copy of each invoice, with supporting documentation, shall be submitted to the address as designated in the order. Invoices for final payment must be so identified and submitted when tasks have been completed and no further charges are to be incurred. These close-out invoices, or a written notification that final invoicing has been completed, must be submitted to the ordering agency within 30 days of Contract completion. A copy of the written acceptance of task completion must be attached to final invoices. If the contractor requires an extension of the 30- day period, a request with supporting rationale must be received prior to the end of the 30-day period. Labor hours of subcontractors shall not be billed at a rate other than the fully burdened hourly rates agreed to in the Contract or at a rate specifically authorized for the Contract as ODCs.

8.3 INVOICE REQUIREMENTS

TIME-AND-MATERIAL (T&M) CLINs (for LABOR)

The contractor may invoice monthly on the basis of cost incurred for the T&M CLINs. The invoice shall include the period of performance covered by the invoice and the CLIN number and title. All hours and costs shall be reported by CLIN element (as shown in Section 1 – Supplies or Services and Price/Costs), by contractor employee, and shall be provided for the current billing month and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. Employee name (current and past employees)
b. Employee company labor category
c. Employee labor category
d. Monthly and total cumulative hours worked
e. Corresponding ceiling rate
f. Cost incurred not billed
g. Current approved forward pricing rate agreement in support of indirect costs billed

FIRM-FIXED PRICE (FFP) CLINS

The contractor may invoice for the FFP CLINs on a monthly basis. The invoice shall include the period of performance or deliverable/progress payment period covered by the invoice and the CLIN number and title. All costs shall be reported by CLIN element and shall be provided for the current invoice and in total from project inception to date. The contractor shall provide the invoice data in spreadsheet form with the following detailed information. The listing shall include separate columns and totals for the current invoice period and the project to date.

a. FFP (insert period of performance or deliverable/progress payment period)
b. Cost incurred not billed

8.4 CLOSE-OUT PROCEDURES

The contractor shall submit a final invoice within 60 calendar days after the end of the performance period. After the final invoice has been paid the contractor shall furnish a completed and signed Release of Claims (GSA Form 1142) to the CO. This release of claims is due within 15 calendar days of final payment.

9.0 CLAUSE

Contract Clauses Incorporated By Reference

FAR 52.227-17 Rights in Data -- Special Works (DEC 2007)

FAR 52.217-5 Evaluation of Options (JUL 1990)

Contract Clauses Incorporated in Full Text

FAR 52.252-1 -- SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation or offer. Also, the full text of a solicitation provision may be accessed electronically at this/these address(es): (http://farsite.hill.af.mil/vffara.htm)

(End of Provision)

FAR 52.252-2 -- CLAUSES INCORPORATED BY REFERENCE (FEB 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es): (http://farsite.hill.af.mil/vffara.htm)

(End of clause)

FAR 52.203-98 -- PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS-REPRESENTATION (DEVIATION 2015-02) (APR 2015)

(a) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Resolution Appropriations Act, 2015 (Pub. L. 113-235), Government agencies are not permitted to use funds appropriated (or otherwise made available) under that or any other Act for contracts with an entity that requires employees or subcontractors of such entity seeking to report fraud, waste, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(b) The prohibition in paragraph (a) of this provision does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(c) Representation. By submission of its offer, the offeror represents that it does not require employees or subcontractors of such entity seeking to report fraud, waste, or abuse to sign internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(End of provision)

FAR 52.203-99 -- PROHIBITION ON CONTRACTING WITH ENTITIES THAT REQUIRE CERTAIN INTERNAL CONFIDENTIALITY AGREEMENTS (DEVIATION 2015-02) (APR 2015)

(a) The Contractor shall not require employees or subcontractors seeking to report fraud, waste, or abuse to sign or comply with internal confidentiality agreements or statements prohibiting or otherwise restricting such employees or subcontractors from lawfully reporting such waste, fraud, or abuse to a designated investigative or law enforcement representative of a Federal department or agency authorized to receive such information.

(b) The contractor shall notify employees that the prohibitions and restrictions of any internal confidentiality agreements covered by this provision are no longer in effect.

(c) The prohibition in paragraph (a) of this clause does not contravene requirements applicable to Standard Form 312, Form 4414, or any other form issued by a Federal department or agency governing the nondisclosure of classified information.

(1) In accordance with section 743 of Division E, Title VII, of the Consolidated and Further Continuing Resolution Appropriations Act, 2015 (Pub. L. 113-235), use of funds appropriated (or otherwise made available) under that or any other Act may be prohibited, if the Government determines that the Contractor is not in compliance with the provisions of this clause.

(2) The Government may seek any available remedies in the event the recipient fails to comply with the provisions of this clause.

(End of clause)

52.224-2 PRIVACY ACT (APR 1984)

(a) The Contractor agrees to -

(1) Comply with the Privacy Act of 1974 (the Act) and the agency rules and regulations issued under the Act in the design, development, or operation of any system of records on individuals to accomplish an agency function when the contract specifically identifies -

(i) The systems of records; and

(ii) The design, development, or operation work that the contractor is to perform;

(2) Include the Privacy Act notification contained in this contract in every solicitation and resulting subcontract and in every subcontract awarded without a solicitation, when the work statement in the proposed subcontract requires the redesign, development, or operation of a system of records on individuals that is subject to the Act; and

(3) Include this clause, including this subparagraph (3), in all subcontracts awarded under this contract which requires the design, development, or operation of such a system of records.

(b) In the event of violations of the Act, a civil action may be brought against the agency involved when the violation concerns the design, development, or operation of a system of records on individuals to accomplish an agency function, and criminal penalties may be imposed upon the officers or employees of the agency when the violation concerns the operation of a system of records on individuals to accomplish an agency function. For purposes of the Act, when the contract is for the operation of a system of records on individuals to accomplish an agency function, the Contractor is considered to be an employee of the agency.

(c)(1) "Operation of a system of records," as used in this clause, means performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.

(2) "Record," as used in this clause, means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and that contains the person's name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a fingerprint or voiceprint or a photograph.

(3) "System of records on individuals," as used in this clause, means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

(End of clause)

52.224-1 PRIVACY ACT NOTIFICATION (APR 1984)

The Contractor will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

(End of clause)